

# THE ARITHMETIC OF CARMICHAEL QUOTIENTS

MIN SHA

ABSTRACT. Carmichael quotients for an integer  $m \geq 2$  are introduced analogous to Fermat quotients, by using Carmichael function  $\lambda(m)$ . Various properties of these new quotients are investigated, such as basic arithmetic properties, Carmichael-Wieferich numbers, non-vanishing, equidistribution, sequences derived from Carmichael quotients and so on. At last, we link Carmichael quotients to the discrete logarithm problem.

## 1. INTRODUCTION

Let  $p$  be a prime and  $a$  an integer not divided by  $p$ , by Fermat's little theorem, the *Fermat quotient* of  $p$  with base  $a$  is defined as follows

$$Q_p(a) = \frac{a^{p-1} - 1}{p}.$$

Moreover, if  $Q_p(a) \equiv 0 \pmod{p}$ , then we call  $p$  a *Wieferich prime* with base  $a$ .

This quotient has been extensively studied from various aspects because of its numerous applications in number theory and computer science, see [8, 11, 20, 21] and references therein. A first comprehensive study of Fermat quotient was published in 1905 by Lerch [17], which was based on the viewpoint of arithmetic. More arithmetic properties were investigated in [3]. For the analytic aspect, such as bounds for the smallest non-vanishing value, exponential sums and character sums, we refer to [6, 23, 24] and references therein. Searching new Wieferich primes always attracts the attentions of mathematicians, see [10, 15, 19] and references therein. More recently, some mathematicians study Fermat quotients from the viewpoint of cryptography and dynamical systems, see [8, 20].

In [4] the authors generalized the definition of Fermat quotient by Euler's theorem. Let  $m \geq 2$  and  $a$  be relatively prime integers, the *Euler quotient* of  $m$  with base  $a$  is defined as follows

$$Q_m(a) = \frac{a^{\varphi(m)} - 1}{m}.$$

Moreover, if  $Q_m(a) \equiv 0 \pmod{m}$ , then we call  $m$  a *Wieferich number* with base  $a$ .

In [4], the authors undertook a careful study of Euler quotients, generalizing many known properties of Fermat quotients discovered by Lerch [17] and Lehmer [16]. More recently, some results about distribution of pseudorandom numbers and vectors derived from Fermat quotients in [20] were extended to Euler quotients in [9]. But much deeper and more extensive properties need to be investigated.

---

2010 *Mathematics Subject Classification.* Primary 11A25; Secondary 11A07.

*Key words and phrases.* Fermat quotient, Carmichael function, Carmichael quotient, Carmichael-Wieferich number.

In fact, there are some other generalizations of Fermat quotients, see [1, 22, 25]. Especially, in [1] the author introduced a quotient like  $\frac{a^e-1}{m}$ , where  $\gcd(a, m) = 1$  and  $e$  is the multiplicative order of  $a$  modulo  $m$ .

In this paper, we introduce a different generalization of Fermat quotient by using Carmichael function. In particular, Proposition 2.1 implies that for applications it is better to use Carmichael quotients to derive pseudorandom numbers and vectors than Euler quotients.

For a positive integer  $m$ , the Carmichael function  $\lambda(m)$  is defined to be the smallest positive integer  $n$  such that

$$a^n \equiv 1 \pmod{m},$$

for every integer  $a$  which is coprime to  $m$ . More explicitly,  $\lambda(1) = 1$ ; for a prime power  $p^\alpha$  we define

$$\lambda(p^\alpha) = \begin{cases} p^{\alpha-1}(p-1) & \text{if } p > 3 \text{ or } \alpha \leq 2, \\ 2^{\alpha-2} & \text{if } p = 2 \text{ and } \alpha \geq 3; \end{cases}$$

and

$$\lambda(m) = \text{lcm}(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \dots, \lambda(p_k^{\alpha_k})),$$

where  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  is the prime factorization of  $m$ .

For every positive integer  $m$ , we have  $\lambda(m) | \varphi(m)$ , and  $\lambda(m) = \varphi(m)$  if and only if  $m \in \{1, 2, 4, p^k, 2p^k\}$ , where  $p$  is an odd prime and  $k \geq 1$ . In addition, if  $m | n$ , we have  $\lambda(m) | \lambda(n)$ .

By the definition of Carmichael function, we have the following definition.

**Definition 1.1.** Let  $m \geq 2$  and  $a$  be relatively prime integers. The quotient

$$C_m(a) = \frac{a^{\lambda(m)} - 1}{m}$$

will be called the *Carmichael quotient* of  $m$  with base  $a$ .

We note that the term ‘‘Carmichael quotient’’ was introduced in [2] to denote a different quotient for a Carmichael number. We do not believe that there is much danger of confusion.

**Definition 1.2.** Let  $m \geq 2$  and  $a$  be relatively prime integers. We call  $m$  a *Carmichael-Wieferich number* with base  $a$  if

$$C_m(a) \equiv 0 \pmod{m}.$$

Before going deeper, in this paper we would like to focus on arithmetic properties of Carmichael quotients. We extend many known results about Fermat quotients or Euler quotients to Carmichael quotients by using the same techniques, such as basic arithmetic properties with special emphasis on congruences, Carmichael-Wieferich numbers, some conditions on  $m$  and  $a$  which ensure that  $C_m(a) \not\equiv 0 \pmod{m}$ , equidistribution of Carmichael quotients and least periods of sequences derived from Carmichael quotient. At last, we link Carmichael quotients to the discrete logarithm problem.

We will indicate the historical remarks mostly by list the literatures in the titles of the results.

## 2. ARITHMETIC OF CARMICHAEL QUOTIENTS

In what follows, we fix  $m \geq 2$  an integer unless stated otherwise.

In this section, we systematically study the basic arithmetic properties of Carmichael quotients and extend many results of [4].

For any integer  $a$  with  $\gcd(a, m) = 1$ , we have  $C_m(a) | Q_m(a)$ . Furthermore, it is straightforward to prove that they have the following relation.

**Proposition 2.1.** *For any  $\gcd(a, m) = 1$ , we have*

$$Q_m(a) \equiv \frac{\varphi(m)}{\lambda(m)} \cdot C_m(a) \pmod{m}.$$

Now we state two fundamental congruences for Carmichael quotients without proof, since it is quite straightforward.

**Proposition 2.2.** (1) *If  $a$  and  $b$  are two integers with  $\gcd(ab, m) = 1$ , then*

$$C_m(ab) \equiv C_m(a) + C_m(b) \pmod{m}.$$

*In particular, if  $b|a$ , then*

$$C_m\left(\frac{a}{b}\right) \equiv C_m(a) - C_m(b) \pmod{m}.$$

(2) *If  $a, k$  are integers with  $\gcd(a, m) = 1$ , and  $\alpha$  is a positive integer, then*

$$C_m(a + km^\alpha) \equiv C_m(a) + \frac{k\lambda(m)}{a} m^{\alpha-1} \pmod{m^\alpha}.$$

The following three corollaries concern some short sums of Carmichael quotients.

**Corollary 2.3** ([27]). *If  $m \geq 3$ , for any  $\gcd(a, m) = 1$  we have*

$$\sum_{k=0}^{m-1} C_m(a + km) \equiv 0 \pmod{m}.$$

*Proof.* From Proposition 2.2 (2), we have

$$\sum_{k=0}^{m-1} C_m(a + km) \equiv \frac{\lambda(m)}{a} \cdot \frac{m(m-1)}{2} \pmod{m}.$$

Notice that  $\lambda(m)$  is even when  $m \geq 3$ . □

**Corollary 2.4.** *If  $m \geq 3$ , we have*

$$\sum_{\substack{a=1 \\ \gcd(a, m)=1}}^{m^2} C_m(a) \equiv 0 \pmod{m}.$$

*Proof.* Notice that

$$\sum_{\substack{a=1 \\ \gcd(a, m)=1}}^{m^2} C_m(a) = \sum_{\substack{a=1 \\ \gcd(a, m)=1}}^m \sum_{k=0}^{m-1} C_m(a + km).$$

□

**Corollary 2.5** ([27]). *For any integer  $k$ , we have*

$$\sum_{\substack{a=km+1 \\ \gcd(a,m)=1}}^{(k+1)m-1} C_m(a) \equiv \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m-1} C_m(a) \pmod{m}.$$

*Proof.* Since

$$\begin{aligned} \sum_{\substack{a=km+1 \\ \gcd(a,m)=1}}^{(k+1)m-1} C_m(a) &\equiv \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m-1} C_m(km+a) \\ &\equiv \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m-1} C_m(a) + k\lambda(m) \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m-1} a^{-1} \\ &\equiv \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m-1} C_m(a) \pmod{m}. \end{aligned}$$

The last equality is derived from  $\sum_{\substack{a=1 \\ \gcd(a,m)=1}}^{m-1} a^{-1} \equiv 0 \pmod{m}$ .  $\square$

The next proposition concerns about some relationships between various  $C_m(a)$  with fixed base  $a$  and different modulus.

**Proposition 2.6.** (1) *If  $\gcd(a, mn) = 1$ , then*

$$C_m(a) | nC_{mn}(a).$$

(2) *If  $\gcd(a, mn) = \gcd(m, n) = 1$ , then*

$$C_{mn}(a) \equiv \frac{\lambda(n)}{n \cdot \gcd(\lambda(m), \lambda(n))} C_m(a) \pmod{m}.$$

(3) ([1, 18]) *If  $\gcd(a, mn) = \gcd(m, n) = 1$ , let  $X$  and  $Y$  be two integers satisfying  $m^2X + n^2Y = 1$ . Then*

$$C_{mn}(a) \equiv \frac{n\lambda(n)}{\gcd(\lambda(m), \lambda(n))} Y C_m(a) + \frac{m\lambda(m)}{\gcd(\lambda(m), \lambda(n))} X C_n(a) \pmod{mn}.$$

*Proof.* (2) By the hypothesis, we have

$$\begin{aligned} C_{mn}(a) &= \frac{a^{\frac{\lambda(m)\lambda(n)}{\gcd(\lambda(m), \lambda(n))}} - 1}{mn} = \frac{(a^{\lambda(m)})^{\frac{\lambda(n)}{\gcd(\lambda(m), \lambda(n))}} - 1}{mn} \\ &\equiv \frac{\lambda(n)(a^{\lambda(m)} - 1)}{mn \cdot \gcd(\lambda(m), \lambda(n))} \pmod{m}. \end{aligned}$$

(3) It suffices to show that the equality is true for modulo  $m$  and modulo  $n$  respectively. But this follows directly from (2).  $\square$

In the following we will give several modulo  $m$  expressions for Carmichael quotients.

For any  $\gcd(a, m) = 1$ , we denote  $\langle a \rangle$  the subgroup of  $(\mathbb{Z}/m\mathbb{Z})^*$  generated by  $a$ , and we denote  $\text{ord}_m a$  the multiplicative order of  $a$  modulo  $m$ . The following expression is so called Lerch's expression [18].

**Proposition 2.7** ([4, 18]). *If  $\gcd(a, m) = 1$  and assume  $n = \text{ord}_m a$ , then*

$$C_m(a) \equiv \frac{\lambda(m)}{n} \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^m \frac{1}{ar} \left\lfloor \frac{ar}{m} \right\rfloor \pmod{m},$$

where  $\lfloor x \rfloor$  denotes the greatest integer  $\leq x$ .

*Proof.* For each  $1 \leq r \leq m$  with  $r \in \langle a \rangle$ , we write  $ar \equiv c_r \pmod{m}$ , with  $1 \leq c_r \leq m$ . Notice that when  $r$  runs through all elements with  $1 \leq r \leq m$  and  $r \in \langle a \rangle$ , so does  $c_r$ . Let  $P$  denote the product of all such integers. If the products and sums are understood to be taken over all  $r$  with  $1 \leq r \leq m$  and  $r \in \langle a \rangle$ , we have

$$P^{\frac{\lambda(m)}{n}} = \prod c_r^{\frac{\lambda(m)}{n}} = \prod \left( ar - m \left\lfloor \frac{ar}{m} \right\rfloor \right)^{\frac{\lambda(m)}{n}} = a^{\lambda(m)} P^{\frac{\lambda(m)}{n}} \prod \left( 1 - \frac{m}{ar} \left\lfloor \frac{ar}{m} \right\rfloor \right)^{\frac{\lambda(m)}{n}},$$

i.e.

$$1 = a^{\lambda(m)} \prod \left( 1 - \frac{m}{ar} \left\lfloor \frac{ar}{m} \right\rfloor \right)^{\frac{\lambda(m)}{n}} \equiv a^{\lambda(m)} \left( 1 - m \sum \frac{1}{ar} \left\lfloor \frac{ar}{m} \right\rfloor \right)^{\frac{\lambda(m)}{n}} \pmod{m^2}.$$

Then we get

$$a^{\lambda(m)} - 1 \equiv a^{\lambda(m)} \frac{m\lambda(m)}{n} \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^m \frac{1}{ar} \left\lfloor \frac{ar}{m} \right\rfloor \pmod{m^2}.$$

Hence, the result follows.  $\square$

In fact, Proposition 2.7 can be obtained directly from [1, Proposition 6].

**Proposition 2.8** ([4, 5, 18]). *If  $\gcd(a, m) = 1$  and assume  $n = \text{ord}_m a$ , then*

$$C_m(a) \equiv \frac{\lambda(m)}{n} \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^m \frac{\beta(r)}{r} \pmod{m},$$

where  $\beta(r)$  denotes the least nonnegative residue of  $-r/m$  modulo  $a$ .

*Proof.* We use the notations in the proof of the above proposition. From the proof of [4, Theorem 2.4], we have  $\lfloor ar/m \rfloor = \beta(c_r)$ . Then the result follows easily.  $\square$

**Proposition 2.9** ([4]). *If  $\gcd(a, m) = 1$ ,  $a \geq 1$  and assume  $n = \text{ord}_m a$ , then*

$$C_m(a) \equiv -\frac{\lambda(m)}{an} \sum_{k=0}^{a-1} \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^{\lfloor km/a \rfloor} r^{\lambda(m)-1} \pmod{m}.$$

*Proof.* We have

$$\begin{aligned}
\sum_{k=0}^{a-1} \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^{\lfloor km/a \rfloor} r^{\lambda(m)-1} &= \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^{m-1} \sum_{\substack{k=0 \\ r \leq \lfloor km/a \rfloor}}^{a-1} r^{\lambda(m)-1} \\
&= \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^{m-1} \left( a - 1 - \left\lfloor \frac{ar}{m} \right\rfloor \right) r^{\lambda(m)-1} \\
&\equiv (a-1) \sum_{i=0}^{n-1} a^i - \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^m \frac{1}{r} \left\lfloor \frac{ar}{m} \right\rfloor \pmod{m} \\
&\equiv - \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^m \frac{1}{r} \left\lfloor \frac{ar}{m} \right\rfloor \pmod{m}.
\end{aligned}$$

According to Proposition 2.7, we get the desired formula.  $\square$

The next proposition extends Lerch's formula of Fermat quotients, the original version see [17], the English exposition see [26].

**Proposition 2.10** ([17]). *Let  $\gcd(a, m) = 1$ ,  $a \geq 1$  and assume  $n = \text{ord}_m a$ . For  $0 \leq k \leq a-1$ , put*

$$s(k, a) = \sum_{\substack{\frac{km}{a} < r < \frac{(k+1)m}{a} \\ r \in \langle a \rangle}} r^{\lambda(m)-1} \equiv \sum_{\substack{\frac{km}{a} < r < \frac{(k+1)m}{a} \\ r \in \langle a \rangle}} \frac{1}{r} \pmod{m}.$$

Then

$$C_m(a) \equiv \frac{\lambda(m)}{an} \sum_{k=0}^{a-1} ks(k, a) \pmod{m}.$$

*Proof.* Since we have

$$\begin{aligned}
\sum_{k=0}^{a-1} ks(k, a) &\equiv \sum_{k=0}^{a-1} \sum_{\substack{\frac{km}{a} < r < \frac{(k+1)m}{a} \\ r \in \langle a \rangle}} \frac{k}{r} \\
&\equiv \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^{m-1} \sum_{\substack{k=0 \\ \frac{km}{a} < r < \frac{(k+1)m}{a}}}^{a-1} \frac{k}{r} \\
&\equiv \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^{m-1} \sum_{\substack{k=0 \\ \frac{ar}{m} - 1 < k < \frac{ar}{m}}}^{a-1} \frac{k}{r} \\
&\equiv \sum_{\substack{r=1 \\ r \in \langle a \rangle}}^{m-1} \frac{1}{r} \left\lfloor \frac{ar}{m} \right\rfloor \pmod{m}.
\end{aligned}$$

The result follows from Proposition 2.7.  $\square$

Now we want to give an identity for Carmichael quotients involving Bernoulli numbers and Bernoulli polynomials.

Recall that Bernoulli polynomials  $B_n(x)$ ,  $n \geq 0$ , can be defined by

$$B_n(x) = \sum_{k=0}^n \binom{n}{k} B_k x^{n-k},$$

where Bernoulli numbers are defined by the generating functions

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} t^k.$$

**Proposition 2.11** ([4]). *If  $\gcd(a, m) = 1$  and  $a \geq 1$ , then we have*

$$C_m(a) = -\frac{a^{\lambda(m)}}{amB_{\lambda(m)}} \sum_{j=0}^{a-1} \left( B_{\lambda(m)}\left(\frac{j}{a}\right) - B_{\lambda(m)} \right).$$

*Proof.* The formula follows easily from the proof of [4, Theorem 3.1].  $\square$

In the last part of this section, we want to factorize Carmichael quotients according to prime factorizations and make reductions by modulo prime factors.

**Proposition 2.12** ([4, 18]). *Let  $m = p_1^{r_1} \cdots p_k^{r_k}$  be the prime factorization of  $m$ , and let  $a$  be an integer with  $\gcd(a, m) = 1$ . For  $1 \leq i \leq k$ , let  $d_i = \lambda(m)/\lambda(p_i^{r_i})$ ,  $m_i = m/p_i^{r_i}$  and  $m'_i \in \mathbb{Z}$  such that  $m_i^2 m'_i \equiv 1 \pmod{p_i^{r_i}}$ . Then*

$$C_m(a) \equiv \sum_{i=1}^k m_i m'_i d_i C_{p_i^{r_i}}(a) \pmod{m}.$$

*Proof.* It suffices to prove for each  $1 \leq j \leq k$ ,

$$C_m(a) \equiv \sum_{i=1}^k m_i m'_i d_i C_{p_i^{r_i}}(a) \pmod{p_j^{r_j}},$$

i.e.

$$C_m(a) \equiv m_j m'_j d_j C_{p_j^{r_j}}(a) \pmod{p_j^{r_j}}.$$

Since we have

$$C_m(a) = \frac{a^{\lambda(p_j^{r_j})d_j} - 1}{m} \equiv \frac{d_j(a^{\lambda(p_j^{r_j})} - 1)}{m} \equiv m_j m'_j d_j C_{p_j^{r_j}}(a) \pmod{p_j^{r_j}},$$

the result follows.  $\square$

**Proposition 2.13.** *Let  $p$  be an odd prime and  $\gcd(a, p) = 1$ . For any two integers  $i$  and  $j$  with  $1 \leq i \leq j$ , we have*

$$C_{p^j}(a) \equiv C_{p^i}(a) \pmod{p^i}.$$

Besides, for  $3 \leq i \leq j$  and  $\gcd(a, 2) = 1$ , we have

$$C_{2^j}(a) \equiv C_{2^i}(a) \pmod{2^{i-1}}.$$

*Proof.* Notice that  $C_{p^i}(a) = Q_{p^i}(a)$  if  $p$  is an odd prime. By [4, Proposition 4.1], for any integer  $k \geq 1$ , we have

$$C_{p^{k+1}}(a) \equiv C_{p^k}(a) \pmod{p^k}.$$

Then the first formula follows.

Since for  $r \geq 3$  we have

$$\begin{aligned} C_{2^{r+1}}(a) - C_{2^r}(a) &\equiv \frac{a^{2^{r-2}} - 1}{2} C_{2^r}(a) \pmod{2^r} \\ &\equiv 0 \pmod{2^{r-1}}, \end{aligned}$$

we can get the other formula.  $\square$

The following corollary, concerning about the relation between Carmichael quotients and Fermat quotients, can be obtained directly from the above two propositions.

**Corollary 2.14.** *Let  $p$  be an odd prime factor of  $m$  and  $\alpha$  be the exact power of  $p$  dividing  $m$ . Suppose that  $d_1 = \frac{\lambda(m)}{\lambda(p^\alpha)}$ ,  $m_1 = m/p^\alpha$  and  $m'_1 \in \mathbb{Z}$  such that  $m_1^2 m'_1 \equiv 1 \pmod{p^\alpha}$ . Then for an integer  $a$  with  $\gcd(a, m) = 1$ , we have*

$$C_m(a) \equiv m_1 m'_1 d_1 Q_p(a) \pmod{p}.$$

In Corollary 2.14, if we furthermore assume that  $p$  satisfies  $\gcd(d_1, p) = 1$ , for example we can choose  $p$  the largest odd prime factor of  $m$ , then  $\gcd(m_1 m'_1 d_1, p) = 1$ . Notice that, in [3] there are various expressions for Fermat quotients modulo  $p$ , especially such expression involving Mirimanoff polynomials, and in [12] some interesting expressions for  $Q_p(2)$  were introduced or proved. So in this case, we can get more expressions for Carmichael quotients modulo  $p$ .

### 3. CARMICHAEL-WIEFERICH NUMBERS

In this section, besides extending some results in [4], we study Carmichael-Wieferich numbers from more aspects, especially Proposition 3.7.

First, we want to deduce some basic facts for Carmichael-Wieferich numbers.

**Proposition 3.1.** *If  $m \geq 3$  and  $1 \leq a \leq m$  with  $\gcd(a, m) = 1$ , then  $m$  can't be a Carmichael-Wieferich number with bases both  $a$  and  $m - a$ .*

*Proof.* Notice that if  $m \geq 3$ , then  $\lambda(m)$  is even. Since we have

$$C_m(m - a) \equiv C_m(a) - \frac{\lambda(m)}{a} \pmod{m},$$

and  $\lambda(m) < m$ . The result follows.  $\square$

**Corollary 3.2.** *There doesn't exist  $m \geq 3$  such that  $m$  is a Carmichael-Wieferich number for any base  $1 \leq a \leq m$ ,  $\gcd(a, m) = 1$ .*

**Corollary 3.3.** *If  $m \geq 3$ , define the set  $S_m = \{a : 1 \leq a \leq m, \gcd(a, m) = 1, m \text{ is a Carmichael-Wieferich number with base } a\}$ . Then  $|S_m| \leq \varphi(m)/2$ .*

From Proposition 2.2 (2), for any  $\gcd(b, m) = 1$ , there exists  $1 \leq a \leq m^2$  with  $b \equiv a \pmod{m^2}$ , such that

$$C_m(b) \equiv C_m(a) \pmod{m}.$$

Hence, if we want to determine with which base  $m$  would be a Carmichael-Wieferich number, we only need to consider  $1 \leq a \leq m^2$ .

By Proposition 2.2, the Carmichael quotient  $C_m(x)$  induces a homomorphism  $C : (\mathbb{Z}/m^2\mathbb{Z})^* \rightarrow (\mathbb{Z}/m\mathbb{Z}, +)$ .

**Proposition 3.4** ([4]). *Let  $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  be the prime factorization of  $m$ . For  $1 \leq r \leq k$ , put*

$$d_r = \begin{cases} \gcd(p_r^{\alpha_r}, 2 \prod_{j=1}^k (p_j - 1)) & \text{if } p_r = 2 \text{ and } \alpha_r \geq 2, \\ \gcd(p_r^{\alpha_r}, \prod_{j=1}^k (p_j - 1)) & \text{otherwise.} \end{cases}$$

*Let  $d = \prod_{r=1}^k d_r$ . Then the image of the homomorphism  $C$  is  $d'\mathbb{Z}/m\mathbb{Z}$ , where  $d' = d / \gcd(\frac{\varphi(m)}{\lambda(m)}, m)$ .*



*Proof.* It is easy to see that  $\gcd(\frac{\varphi(m)}{\lambda(m)}, m) | d$ . Notice that for any two non-zero integers  $n_1$  and  $n_2$ , we have

$$n_1\mathbb{Z}/m\mathbb{Z} = n_2\mathbb{Z}/m\mathbb{Z} \quad \text{if and only if} \quad \gcd(n_1, m) = \gcd(n_2, m).$$

Then the result follows from Proposition 2.1 and [4, Proposition 4.4].  $\square$

**Corollary 3.5** ([4]). *The homomorphism  $C$  has kernel of order  $d'\varphi(m)$ , where  $d'$  is defined in Proposition 3.4.*

**Corollary 3.6.** *Define the set  $T_m = \{a : 1 \leq a \leq m^2, \gcd(a, m) = 1, m \text{ is a Carmichael-Wieferich number with base } a\}$ . Then  $|T_m| = d'\varphi(m)$ , where  $d'$  is defined in Proposition 3.4.*

The following proposition implies that Carmichael-Wieferich numbers are rare.

**Proposition 3.7.** *We have  $\lim_{m \rightarrow \infty} \frac{|T_m|}{\varphi(m^2)} = 0$ .*

*Proof.* For any  $m \geq 2$ , we denote the variable  $d$  in Proposition 3.4 by  $D_m$ . We have  $\frac{|T_m|}{\varphi(m^2)} \leq \frac{D_m}{m}$ . So it suffices to show that  $\lim_{m \rightarrow \infty} \frac{D_m}{m} = 0$ .

For primes  $p$ , we have

$$\lim_{p \rightarrow \infty} \frac{D_p}{p} = \lim_{p \rightarrow \infty} \frac{1}{p} = 0.$$

So  $\liminf_{m \rightarrow \infty} \frac{D_m}{m} = 0$ .

Suppose that  $\limsup_{m \rightarrow \infty} \frac{D_m}{m} \neq 0$ . Then there exists a subsequence  $\{\frac{D_{n_i}}{n_i}\}$  such that

$$\lim_{i \rightarrow \infty} \frac{D_{n_i}}{n_i} = \limsup_{m \rightarrow \infty} \frac{D_m}{m} \neq 0.$$

Let  $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  be the prime factorization of  $m$ . Put  $\beta_m = \max\{\alpha_1, \dots, \alpha_k\}$ . Here we use the notations in Proposition 3.4. For each  $1 \leq r \leq k$ , we have  $\frac{D_m}{m} \leq d_r/p_r^{\alpha_r}$ . In particular, if  $p_k$  is the largest prime factor of  $m$ , then  $\frac{D_m}{m} \leq 2/p_k^{\alpha_k}$ .

For each  $n_i$ , let  $p_i$  be the largest prime factor of  $n_i$ , we replace  $\beta_{n_i}$  by  $\beta_i$ . Since  $\frac{D_{n_i}}{n_i} \leq \frac{2}{p_i^{\beta_i}}$ , there must exist an integer  $q$  such that  $p_i < q$ , for all  $i \geq 1$ . Put  $\gamma = 2 \prod_{\substack{2 \leq p < q \\ p \text{ prime}}} (p-1)$ . Then we have  $\frac{D_{n_i}}{n_i} \leq \frac{\gamma}{2^{\beta_i}}$ . Notice that  $n_i \rightarrow \infty$  when  $i \rightarrow \infty$ ,

we must have  $\beta_i \rightarrow \infty$  as  $i \rightarrow \infty$ . Hence we have  $\lim_{i \rightarrow \infty} \frac{D_{n_i}}{n_i} = 0$ . Contradiction.

So we have  $\limsup_{m \rightarrow \infty} \frac{D_m}{m} = 0$ .  $\square$

In the following we want to characterize all Carmichael-Wieferich numbers by means of Wieferich primes.

Let  $p$  be a prime and  $a$  an integer with  $p \nmid a$ . Put

$$\begin{aligned} \sigma(a, p) &= \text{ord}_p(a^{p-1} - 1) - 1 \quad \text{if } p \text{ is odd,} \\ \sigma(a, 2) &= \begin{cases} \text{ord}_2(a-1) - 1 & \text{if } a \equiv 1 \pmod{4}, \\ \text{ord}_2(a+1) - 1 & \text{if } a \equiv 3 \pmod{4}. \end{cases} \end{aligned}$$

**Proposition 3.8** ([4]). *Let  $\gcd(a, m) = 1$ , and  $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  be the prime factorization of  $m \geq 3$ . Let  $1 \leq j \leq k$ ,  $p = p_j$  and  $\alpha = \alpha_j$ . If  $p \neq 2$  or  $\alpha \leq 2$ , put*

$$n = \begin{cases} 0 & \text{if } \text{ord}_p \text{lcm}(p_1 - 1, \dots, p_k - 1) \leq \alpha - 1, \\ \text{ord}_p \text{lcm}(p_1 - 1, \dots, p_k - 1) - \alpha + 1 & \text{otherwise;} \end{cases}$$

otherwise if  $p = 2$  and  $\alpha > 2$ , put

$$n = \begin{cases} 0 & \text{if } \text{ord}_p \text{lcm}(p_1 - 1, \dots, p_k - 1) \leq \alpha - 2, \\ \text{ord}_p \text{lcm}(p_1 - 1, \dots, p_k - 1) - \alpha + 2 & \text{otherwise.} \end{cases}$$

Moreover, put

$$e(m, p) = \begin{cases} n & \text{if } p \neq 2 \text{ or } \alpha \leq 2, \\ n - 1 & \text{otherwise.} \end{cases}$$

Then we have

$$\text{ord}_p C_m(a) = e(m, p) + \sigma(a, p).$$

*Proof.* Put  $b = a^{p^n \lambda(p^\alpha)}$ . Then  $\lambda(m) = p^n \lambda(p^\alpha) X$ , where  $X$  is an integer with  $p \nmid X$ . Applying the method in the proof of [4, Proposition 5.4], we get the desired result.  $\square$

The next proposition, a criterion for a number  $m$  being a Carmichael-Wieferich number, follows easily from the above proposition.

**Proposition 3.9** ([4]). *Let  $\gcd(a, m) = 1$ , and  $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  be the prime factorization of  $m \geq 3$ . Then the following statements are equivalent:*

- (1)  *$m$  is a Carmichael-Wieferich number with base  $a$ ,*
- (2)  *$e(m, p_j) + \sigma(a, p_j) \geq \alpha_j$ , for any  $1 \leq j \leq k$ .*

**Corollary 3.10** ([4]). *Let  $m_1$  and  $m_2$  be relatively prime Carmichael-Wieferich numbers with base  $a$ . Then  $m_1 m_2$  is a Carmichael-Wieferich number with base  $a$ .*

Although it is known that Wieferich primes exist for many different bases, see [19], the following problem is still open.

*Whether Wiererich primes exist for all bases?*

**Proposition 3.11.** *For a non-zero integer  $a$ , if there exists a Carmichael-Wieferich number  $m$  with base  $a$  and  $m$  has an odd prime factor, then there exists a Wieferich prime with base  $a$ .*

*Proof.* Let  $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  be the prime factorization of  $m$  with  $p_1 < p_2 < \cdots < p_k$ . Since  $m$  is a Carmichael-Wieferich number with base  $a$ , we have  $\sigma(a, p_k) \geq \alpha_k \geq 1$ . Notice that  $p_k$  is an odd prime, so  $p_k$  is a Wieferich prime with base  $a$ .  $\square$

**Example 3.12.** From Table 1 of [19], 3 and 7 are two Wieferich primes with base 19. It is straightforward to see that 2 is not a Wieferich prime with base 19. By [4, Theorem 5.5],  $m = 2^2 \cdot 3 \cdot 7$  is a Wieferich number with base 19. But by Proposition 3.9,  $m$  is not a Carmichael-Wieferich number with base 19.

#### 4. NON-VANISHING OF CARMICHAEL QUOTIENTS

In this section, we want to extend some results in [14] to Carmichael quotients, that is deriving various conditions on  $m$  and  $a$  which ensure that  $C_m(a) \not\equiv 0 \pmod{m}$ .

In this section, we suppose that  $p_m$  is the largest prime factor of  $m$ .

The following proposition is fundamental for this section, the original result see [14, Theorem].

**Proposition 4.1** ([14]). *Let  $\gcd(a, m) = 1$ , and suppose  $a \geq 2$ . Let  $r \geq 1$  be such that  $\gcd(r, m) = 1$  and  $a^r \equiv \pm 1 \pmod{m}$ . If  $t$  is defined by  $a^r = \pm 1 + tm$ , then we have*

$$C_m(a) \equiv \pm \frac{t}{r} \lambda(m) \pmod{m}.$$

*Proof.* It suffices to notice that  $rC_m(a) \equiv C_m(a^r) \pmod{m}$  and apply Proposition 2.2 (2).  $\square$

**Corollary 4.2** ([14]). *Let  $\gcd(a, m) = 1$ , put*

$$D = \frac{a^{sk} \mp 1}{a^k \mp 1} = a^{(s-1)k} \pm a^{(s-2)k} + \cdots + a^{2k} \pm a^k + 1,$$

*where  $a \geq 2$ ,  $s, k \geq 1$  with  $\gcd(sk, m) = 1$ , and  $s$  is odd in the case of the bottom choice of sign. If  $D$  can be factored as  $D = md$ , then*

$$C_m(a) \equiv \pm \frac{d(a^k \mp 1)}{sk} \lambda(m) \pmod{m}.$$

**Corollary 4.3** ([14]). *If  $a, s, k$  and  $D$  are as above, moreover  $p_m \nmid a^k \mp 1$ , and if  $m$  is a linear factor of  $D$ , that is  $m \mid D$  but  $m^2 \nmid D$ , then  $C_m(a) \not\equiv 0 \pmod{m}$ .*

*Proof.* It suffices to notice that  $\lambda(m) \mid \varphi(m)$  and  $p_m \nmid d(a^k \mp 1)\varphi(m)$ .  $\square$

Given  $a \geq 2$ , every odd integer  $m$ , satisfying  $\gcd(a, m) = \gcd(a-1, m) = 1$ , divides  $D = a^{\lambda(m)-1} + \cdots + a + 1$  since  $a^{\lambda(m)} \equiv 1 \pmod{m}$ . Furthermore, if  $\gcd(\lambda(m), m) = 1$ , then Corollary 4.3 says that such expression are divided linearly by  $m$  or not, according to whether  $C_m(a) \not\equiv 0 \pmod{m}$ .

The condition  $\gcd(\lambda(m), m) = 1$  is equivalent to  $\gcd(\varphi(m), m) = 1$ . So this condition requires that  $m$  only has linear prime factors. There are infinitely many composite number  $m$  satisfying  $\gcd(\varphi(m), m) = 1$ . For example, first we choose a big prime  $p_2$ , and then choose a prime  $p_1 < p_2$  such that  $\gcd(p_1, p_2 - 1) = 1$ , then put  $m = p_1 p_2$ .

Now we want to give some explicit kinds of non-vanishing Carmichael quotients  $\pmod{m}$ .

**Proposition 4.4** ([14]). *Suppose that  $\gcd(\lambda(m), m) = 1$ . If  $0 < a < m$  and the multiplicative order of  $a$  modulo  $m$  is 2, then  $C_m(a) \not\equiv 0 \pmod{m}$ .*

*Proof.* Suppose that  $a^2 = 1 + tm$ . Since  $\gcd(2, m) = 1$ ,  $C_m(a) \equiv t\lambda(m)/2 \pmod{m}$ . Notice that  $a^2 < m^2$ , then  $t < m$ . Then we can get the result.  $\square$

If  $p_m$  is a linear odd prime factor of  $m$ , for ensuring  $C_m(a) \not\equiv 0 \pmod{m}$ , it suffices to satisfy  $C_m(a) \not\equiv 0 \pmod{p_m}$ . By Corollary 2.14,  $C_m(a) \not\equiv 0 \pmod{p_m}$  if and only if  $Q_{p_m}(a) \not\equiv 0 \pmod{p_m}$ . Hence, we can apply the results in [14] to construct various explicit kinds of non-vanishing Carmichael quotients  $\pmod{m}$ .

## 5. EQUIDISTRIBUTION OF CARMICHAEL QUOTIENTS

The result of [13, Theorem 2] shows that Fermat quotients are uniformly distributed modulo  $p$  for  $1 \leq a < p$ . Theorem 4.1 in [27] generalized this result to Euler quotients. For Carmichael quotients we can get a similar result following the method in [13]. For the sake of completeness, we present the proof.

**Proposition 5.1** ([13, 27]). *For any integer  $a$  with  $\gcd(a, m) = 1$  and any real number  $\epsilon > 0$ , we have*

$$\sum_{\substack{M < n \leq M+N \\ \gcd(n, m)=1}} \exp\left(\frac{aC_m(n)}{m}\right) \ll N^{\frac{1}{2}} m^{\frac{3}{8}+\epsilon},$$

uniformly for  $M, N \geq 1$ , the implied constant depending only on  $\epsilon$ .

*Proof.* We define an arithmetic function  $\chi(n)$  as follows,

$$\chi(n) = \begin{cases} 0 & \gcd(n, m) \neq 1, \\ \exp\left(\frac{aC_m(n)}{m}\right) & \gcd(n, m) = 1. \end{cases}$$

By Proposition 2.2 (1) and noticing that  $\chi(m+1) \neq 1$ , we have  $\chi$  is indeed a non-principle Dirichlet character modulo  $m^2$ .

Hence we have

$$\sum_{\substack{M < n \leq M+N \\ \gcd(n, m)=1}} \exp\left(\frac{aC_m(n)}{m}\right) = \sum_{M < n \leq M+N} \chi(n).$$

Then the desired result follows from an estimate in [7, Theorem 2].  $\square$

## 6. SEQUENCES DERIVED FROM CARMICHAEL QUOTIENTS

In this section we will define two periodic sequences by Carmichael quotients and determine their least (positive) periods following the method in the proof of [9, Proposition 2.1]. In fact, here it is more complicated when  $m$  is even.

In this section, let  $m = p_1^{r_1} \cdots p_k^{r_k}$  be the prime factorization of  $m$ . For each  $1 \leq i \leq k$ , put  $m_i = m/p_i^{r_i}$ , and let  $0 \leq w_i \leq r_i$  be defined by  $p_i^{w_i} = \gcd(\lambda(m)/\lambda(p_i^{r_i}), p_i^{r_i})$ . Furthermore, for each  $i$ , if  $p_i | a$ , set  $C_{p_i^{r_i}}(a) = 0$ .

We will define a sequence  $\{a_n\}$  following the manner in [9].

For every integer  $n \geq 1$ , by Proposition 2.12,  $a_n$  is defined as the unique integer with

$$a_n \equiv \sum_{i=1}^k \frac{m_i m'_i \lambda(m)}{\lambda(p_i^{r_i})} C_{p_i^{r_i}}(n) \pmod{m}, \quad 0 \leq a_n \leq m-1,$$

where  $m'_i \in \mathbb{Z}$  such that  $m_i^2 m'_i \equiv 1 \pmod{p_i^{r_i}}$  for all  $1 \leq i \leq k$ . So if  $\gcd(n, m) = 1$ , we have  $a_n \equiv C_m(n) \pmod{m}$ .

By Proposition 2.2 (2),  $m^2$  is a period of  $\{a_n\}$ . We denote its least period by  $T$ . For each  $1 \leq i \leq k$ , let  $T_i$  be the least period of  $\{a_n\}$  modulo  $p_i^{r_i}$ . Then obviously we have

$$T = \text{lcm}(T_1, \dots, T_k).$$

So to determine  $T$ , it suffices to compute  $T_i$  for each  $i$ .

For all  $1 \leq i \leq k$ , we have

$$(6.1) \quad a_n \equiv \frac{\lambda(m)}{m_i \lambda(p_i^{r_i})} C_{p_i^{r_i}}(n) \pmod{p_i^{r_i}}.$$

So  $T_i$  equals to the least period of  $\{C_{p_i^{r_i}}(n)\}$  modulo  $p_i^{r_i-w_i}$ . Then we also denote  $T_i$  the least period of  $\{C_{p_i^{r_i}}(n)\}$  modulo  $p_i^{r_i-w_i}$  without confusion. In the sequel, we will analyze case by case to calculate  $T_i$ .

**Lemma 6.1.** *If  $w_i = r_i$ , then  $T_i = 1$ .*

*Proof.* Since in this case we have  $C_{p_i^{r_i}}(n) \equiv 0 \pmod{p_i^{r_i-w_i}}$  for all  $n \geq 1$ .  $\square$

**Lemma 6.2.** *If  $p_i > 2$  and  $w_i < r_i$ , then  $T_i = p_i^{r_i-w_i+1}$ .*

*Proof.* Combining Proposition 2.13 and Proposition 2.2 (2), for all  $n$  with  $\gcd(n, p_i) = 1$ , we have

$$C_{p_i^{r_i}}(n + ap_i^{r_i-w_i}) \equiv C_{p_i^{r_i}}(n) - an^{-1}p_i^{r_i-w_i-1} \pmod{p_i^{r_i-w_i}}.$$

Hence  $T_i = p_i^{r_i-w_i+1}$ .  $\square$

**Lemma 6.3.** *If  $p_i = 2$  and  $w_i = 0$ , then*

$$T_i = \begin{cases} 4 & r_i = 1, \\ 8 & r_i = 2, \\ 2^{r_i+2} & r_i \geq 3 \end{cases}$$

*Proof.* Notice that for  $\gcd(n, m) = 1$ , we have

$$C_{2^{r_i}}(n + a2^{r_i}) \equiv C_{2^{r_i}}(n) + an^{-1}\lambda(2^{r_i}) \pmod{2^{r_i}}.$$

$\square$

**Lemma 6.4.** *For  $r \geq 3$ , the least period of  $\{C_{2^{r+1}}(n)\}$  modulo  $2^r$  is  $2^{r+2}$ .*

*Proof.* For  $r \geq 3$  and  $\gcd(n, 2) = 1$ , we have  $C_{2^{r+1}}(n) = \frac{n^{2^r-2}+1}{2}C_{2^r}(n)$ . Then

$$\begin{aligned} C_{2^{r+1}}(n + a2^r) - C_{2^{r+1}}(n) &\equiv \frac{n^{2^r-2}+1}{2} (C_{2^r}(n + a2^r) - C_{2^r}(n)) \\ &\equiv \frac{n^{2^r-2}+1}{2} \cdot an^{-1}2^{r-2} \\ &\equiv an^{-1}2^{r-2} \pmod{2^r}. \end{aligned}$$

So we can get the desired result.  $\square$

**Lemma 6.5.** *If  $p_i = 2$  and  $3 \leq r_i - w_i < r_i$ , then  $T_i = 2^{r_i-w_i+2}$ .*

*Proof.* By Proposition 2.13, for  $\gcd(n, 2) = 1$ , we have

$$C_{2^{r_i}}(n) \equiv C_{2^{r_i-w_i+1}}(n) \pmod{2^{r_i-w_i}}.$$

Then the result follows directly from Lemma 6.4.  $\square$

**Lemma 6.6.** *If  $p_i = 2$ ,  $r_i \geq 3$  and  $1 \leq r_i - w_i \leq 2$ , then  $T_i = 2^{r_i-w_i+2}$ .*

*Proof.* From Proposition 2.13, for  $\gcd(n, 2) = 1$ , we have

$$C_{2^{r_i}}(n) \equiv C_{2^3}(n) \pmod{2^2}.$$

So  $T_i$  equals to the least period of  $\{C_{2^3}(n)\}$  modulo  $2^{r_i-w_i}$ . Noticing that  $2^6$  is a period of  $\{C_{2^3}(n)\}$  modulo  $2^{r_i-w_i}$ , then one can calculate directly to check the result.  $\square$

**Lemma 6.7.** *If  $p_i = 2$ ,  $r_i = 2$  and  $r_i - w_i = 1$ , then  $T_i = 1$ .*

We summarize the above results in the following proposition.

**Proposition 6.8.** *For each  $1 \leq i \leq k$ , if  $p_i$  is an odd prime, then*

$$T_i = \begin{cases} 1 & w_i = r_i, \\ p_i^{r_i - w_i + 1} & w_i < r_i; \end{cases}$$

*otherwise if  $p_i = 2$ , then*

$$T_i = \begin{cases} 1 & w_i = r_i, \\ 4 & r_i = 1, w_i = 0, \\ 8 & r_i = 2, w_i = 0, \\ 1 & r_i = 2, w_i = 1, \\ 2^{r_i - w_i + 2} & r_i \geq 3, w_i < r_i. \end{cases}$$

*In particular,  $T = T_1 \cdots T_k$ .*

Now we want to define a new sequence  $\{b_n\}$ , which is much simpler but has the same least period as  $\{a_n\}$ .

For an integer  $n \geq 1$  with  $\gcd(n, m) = 1$ ,  $b_n$  is defined to be the unique integer with

$$b_n \equiv C_m(n) \pmod{m}, \quad 0 \leq a_n \leq m-1;$$

and we also define

$$b_n = 0, \quad \text{if } \gcd(n, m) \neq 1.$$

Since  $b_n$  also satisfies (6.1) for all  $\gcd(n, m) = 1$ , the least period of  $\{b_n\}$  equals to that of  $\{a_n\}$ .

## 7. CARMICHAEL QUOTIENTS AND THE DISCRETE LOGARITHM PROBLEM

We have known that for an integer  $m \geq 2$ , the Carmichael quotient  $C_m(x)$  induces a homomorphism

$$C : (\mathbb{Z}/m^2\mathbb{Z})^* \rightarrow (\mathbb{Z}/m\mathbb{Z}, +), \quad x \rightarrow C_m(x).$$

Assume that  $g$  is an element of  $(\mathbb{Z}/m^2\mathbb{Z})^*$  of order  $\lambda(m^2)$ . Then we get a homomorphism, denoted by  $c$ ,

$$c : \langle g \rangle \rightarrow (\mathbb{Z}/m\mathbb{Z}, +), \quad g^k \rightarrow C_m(g^k),$$

where  $\langle g \rangle$  is the subgroup of  $(\mathbb{Z}/m^2\mathbb{Z})^*$  generated by  $g$ .

Notice that  $m \mid \lambda(m^2)$ , we can define another homomorphism, denoted by  $\log$ ,

$$\log : \langle g \rangle \rightarrow (\mathbb{Z}/m\mathbb{Z}, +), \quad g^k \rightarrow k.$$

For any two homomorphisms  $\varphi : \langle g \rangle \rightarrow \langle g \rangle, g \rightarrow g^n$  and  $\psi : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}, x \rightarrow ax$ , it is easy to get the following proposition.

**Proposition 7.1.** *The following diagram is commutative*

$$\begin{array}{ccc} \langle g \rangle & \xrightarrow{c} & \mathbb{Z}/m\mathbb{Z} \\ \downarrow \varphi & & \downarrow \psi \\ \langle g \rangle & \xrightarrow{\log} & \mathbb{Z}/m\mathbb{Z} \end{array}$$

*if and only if  $aC_m(g) \equiv n \pmod{m}$ .*

Here, our main interest is the case that  $m$  is an odd prime  $p$ . In this case, we replace the notations  $C_p$  and  $c$  by  $Q_p$  and  $q$  respectively by convention.

We assume  $g$  is a primitive element of  $(\mathbb{Z}/p\mathbb{Z})^*$ . If  $g^{p-1} \not\equiv 1 \pmod{p^2}$ , then  $g$  is also a primitive element of  $(\mathbb{Z}/p^2\mathbb{Z})^*$ . Otherwise,  $g + p$  is a primitive element of  $(\mathbb{Z}/p^2\mathbb{Z})^*$ .

Hence, for simplicity we assume that  $g$  is a primitive element both in  $(\mathbb{Z}/p\mathbb{Z})^*$  and in  $(\mathbb{Z}/p^2\mathbb{Z})^*$ .

Notice that  $p \nmid Q_p(g)$ . Since if  $p \mid Q_p(g)$ , the image of  $q$  is 0. We have the following proposition.

**Proposition 7.2.** *For any given homomorphism*

$$\varphi_n : (\mathbb{Z}/p^2\mathbb{Z})^* \rightarrow (\mathbb{Z}/p^2\mathbb{Z})^*, \quad u \rightarrow u^n,$$

*there exists an unique homomorphism*

$$\psi_n : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}, \quad x \rightarrow ax,$$

*such that the following diagram is commutative.*

$$\begin{array}{ccc} (\mathbb{Z}/p^2\mathbb{Z})^* & \xrightarrow{q} & \mathbb{Z}/p\mathbb{Z} \\ \downarrow \varphi_n & & \downarrow \psi_n \\ (\mathbb{Z}/p^2\mathbb{Z})^* & \xrightarrow{\log} & \mathbb{Z}/p\mathbb{Z} \end{array}$$

*Furthermore,  $a \equiv nQ_p(g)^{-1} \pmod{p}$ .*

In particular, if we choose  $n$  with  $p \nmid n$ , then for any  $u \in (\mathbb{Z}/p^2\mathbb{Z})^*$ , we have

$$(7.1) \quad \log u \equiv n^{-1}aQ_p(u) \pmod{p}.$$

Notice that the discrete logarithm problem modulo  $p$  and that modulo  $p^2$  are equivalent. Although nowadays we have no efficient algorithms to solve the discrete logarithm problem modulo  $p^2$ , i.e. calculating  $\log u$ , we can have an efficient algorithm to calculate the value of  $\log u$  modulo  $p$  by using (7.1).

## 8. ACKNOWLEDGEMENTS

We would like to thank Professor A. Winterhof for sending us their recent work [9]. We also would like to thank the referee for the careful reading and the valuable suggestions.

## REFERENCES

- [1] T. Agoh, *Fermat and Euler type quotients*, C. R. Math. Rep. Acad. Sci. Canada **17** (1995), 159-164.
- [2] T. Agoh, *On Giuga's conjecture*, Manuscripta Math. **87** (1995), 501-510.
- [3] T. Agoh, *On Fermat and Wilson Quotients*, Expo. Math. **14** (1996), 145-170.
- [4] T. Agoh, K. Dilcher and L. Skula, *Fermat Quotients for Composite Moduli*, J. Number Theory **66** (1997), 29-50.
- [5] H.F. Baker, *Remark on the Eisenstein-Sylvester extension of Fermat's theorem*, Proc. London Math. Soc. **4** (1906), 131-135.
- [6] J. Bourgain, K. Ford, S. Konyagin and I. Shparlinski, *On the divisibility of Fermat quotients*, Michigan Math. J. **59** (2010), 313-328.
- [7] D.A. Burgess, *On character sums and L-functions II*, Proc. London Math. Soc. (13) (1963), 524-536.
- [8] Z. Chen, A. Ostafe and A. Winterhof, *Structure of Pseudorandom Numbers Derived from Fermat Quotients*, Lect. Notes in Comp. Sci. 6087, Springer, Berlin, 2010, 73-85.

- [9] Z. Chen and A. Winterhof, *On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients*, Int. J. Number Theory, to appear.
- [10] R. Ernvall and T. Metsänkylä, *On the  $p$ -divisibility of Fermat quotients*, Math. Comp. **66** (1997), 1353-1365.
- [11] A. Granville, *Some conjectures related to Fermat's Last Theorem*, Number Theory, W. de Gruyter, NY, 1990, 177-192.
- [12] A. Granville, *The square of the Fermate quotients*, Integers **4** (2004), A22.
- [13] D.R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, in Analytic Number Theory, Vol. 2, Progr. Math. 139, Birkhäuser Boston, 1996.
- [14] W. Johnson, *On the nonvanishing of Fermat quotients (mod  $p$ )*, J. Reine Angew. Math. **292** (1977), 196-200.
- [15] W. Keller and J. Richstein, *Solutions of the congruences  $a^{p-1} \equiv 1 \pmod{p^r}$* , Math. Comp. **74** (2005), 927-936.
- [16] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. **39** (1938), 350-360.
- [17] M. Lerch, *Zur Theorie es Fermatschen Quotienten  $(a^{p-1} - 1)/p = q(a)$* , Math. Ann. **60** (1905), 471-490.
- [18] M. Lerch, *Sur les théorèmes de Sylvester concernant le quotient de Fermat*, C. R. Acad. Sci. Paris **142** (1906), 35-38.
- [19] P.L. Montgomery, *New solutions of  $a^{p-1} \equiv 1 \pmod{p^2}$* , Math. Comp. **61** (1993), 361-363.
- [20] A. Ostafe and I. Shparlinski, *Pseudorandomness and dynamics of Fermat quotients*, SIAM J. Discr. Math. **25** (2011), 50-71.
- [21] P. Ribenboim, *Thirteen lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.
- [22] J. Sauerberg and L. Shu, *Fermat Quotients over Function Fields*, Finite Fields Th. App. **3** (1997), 275-286.
- [23] I. Shparlinski, *Fermat quotients: Exponential sums, value set and primitive roots*, Bull. London Math. Soc., to appear.
- [24] I. Shparlinski, *Character sums with Fermat quotients*, Quart. J. Math., to appear.
- [25] L. Skula, *Fermat and Wilson quotients for  $p$ -adic integers*, Acta Mathematica Universitatis Ostraviensis **6** (1998), 167-181.
- [26] L. Skula, *A note on some relations among special sums of reciprocals modulo  $p$* , Math. Slovaca **58** (2008), 5-10.
- [27] I. Solan, *Some properties of the Euler quotient matrix*, Integers **6** (2006), A36.

INSTITUT DE MATHÉMATIQUES DE BORDEAUX, UNIVERSITE BORDEAUX 1 , 33405 TALENCE  
CEDEX, FRANCE

*E-mail address:* shamin2010@gmail.com